## REMARKS

Claims 1, 3, 6, 8, 10-26, 28-38, 41-43, and 45-53 are pending in the present application. By this amendment, claims 1, 3, 6, 10-19, 21, 23, 26, 30-38, 41-43, and 45-53 are amended, and claims 2, 4-5, 7, 27, and 39 are canceled without prejudice or disclaimer. Support for the amendments can be found at least at page 11, line 8 through page 12, line 31 and page 17, line 7 through page 18, line 19 of the specification. Applicant respectfully requests reconsideration of the present claims in view of the above amendments and following remarks.

I. Formal Matters

Interview Summary

A telephonic interview occurred between Examiner Lemma and the undersigned, Jodi Hartman, on September 6, 2007. During the interview, Examiner Lemma and the undersigned discussed potential amendments to the claims, similar to those set forth above, which Examiner Lemma agreed would likely overcome the rejections in view of the references cited. Examiner Lemma noted that another search would need to be performed.

II. Claim Rejections

Claim Rejections Under 35 U.S.C. §101

Claims 1-8, 10-15, 31-39, 41-43, 45-49 and 52-53 are rejected under 35 U.S.C. §101 because the subject matter is allegedly directed to non-statutory subject matter. As noted above, claims 2, 4-5, 7, and 39 are canceled without prejudice or disclaimer, rendering this rejection moot with regard to those claims. Applicant respectfully traverses this rejection.

A. Claims 1, 3, 6, 8, 10-15, and 48-49

The Office Action notes that claims 1, 3, 6, 8, 10-15, and 48-49 are directed to a system for providing network-based firewall policy configuration and facilitation associated with a firewall and include recitations that allegedly raise a question as to whether the claims are directed merely to an abstract idea that is not tied to a technological art, environment or machine which would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C. §101. Although Applicant respectfully traverses this rejection, claims 1, 3, 6, 8, 10-15, and 48-49 are amended to recite a

processor operative to perform the recitations of the claims. As described in the specification at page 5, lines 28-33, the processor is a hardware device. Therefore, claims 1, 3, 6, 8, 10-15, and 48-49 are directed to statutory subject matter. Accordingly, withdrawal of this rejection is respectfully requested.

B. Claims 31-38, 41-43, 45-47, and 52-53

The Office Action notes that claims 31-38, 41-43, 45-47, and 52-53 are directed to a computer-readable medium for providing network-based firewall policy configuration and facilitation associated with a firewall and allegedly raise a question as to whether the claims are directed merely to an abstract idea that is not tied to a technological art, environment or machine which would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C. §101. Although Applicant respectfully traverses this rejection, claims 31-38, 41-43, 45-47, and 52-53 are amended to recite "a computer-readable storage medium" which is more clearly directed to statutory subject matter. Accordingly, withdrawal of this rejection is respectfully requested.

Claim Rejections Under 35 U.S.C. §102

Claims 1-8, 10-13, 16-28, 31-39, 41-43 and 45 are rejected under 35 U.S.C. 102(a) as being anticipated by an article written with the title "Understanding Security Policies" (hereinafter "Cisco"). As noted above, claims 2, 4-5, 7, and 39 are canceled without prejudice or disclaimer, rendering this rejection moot with regard to those claims. This rejection is respectfully traversed.

As amended, claim 1 recites that a system for providing network-based firewall policy configuration and facilitation associated with a firewall comprises a processor, functionally coupled to the memory device, the processor being responsive to computer-executable instructions contained in the program and operative to determine whether the application includes one or more questionable packets, and if the application is determined to include one or more questionable packets, modify the user's firewall policy to allow packets associated with the application determined not to be questionable to pass through the firewall unblocked and exclude the one or more questionable packets associated with the application from modification of the

user's firewall policy such that the one or more questionable packets are blocked from passing through the firewall.

Cisco does not teach, suggest, or describe a system for providing network-based firewall policy configuration and facilitation associated with a firewall as recited by claim 1. On the contrary, Cisco describes a firewall (Cisco Centri Firewall) operative to filter session attempts by evaluating the incoming request to start a new session against session controls and responses defined by a security policy to determine whether to allow the new session. Cisco further describes that the session controls used by the Cisco Centri Firewall to determine whether to allow a new session may be run-time session controls which are session controls that can be modified at the time the session request is received by the firewall and can either apply to all communications or to a specific network service.

This is not analogous to the system recited by claim 1 because Cisco fails to teach, suggest, or describe a processor operative to determine whether a session includes one or more questionable packets, and if the session is determined to include one or more questionable packets, modify either the security policy or the run-time session controls to allow packets associated with the session determined not to be questionable to pass through the firewall unblocked and exclude the one or more questionable packets associated with the session from modification of the security policy or the run-time session controls such that the one or more questionable packets are blocked from passing through the firewall. Instead, Cisco describes that the run-time session controls can be modified at the time the session request is received by the firewall but fails to teach, suggest, or describe a processor operative to modify the run-time session controls to allow packets associated with the session determined not to be questionable to pass through the firewall unblocked and exclude the one or more questionable packets associated with the session from modification of the run-time session controls such that the one or more questionable packets are blocked from passing through the firewall.

For at least the reasons given above, claim 1 is allowable over Cisco. Since claims 3, 6, 8, and 10-13 depend from claim 1 and recite further claim features, Applicant respectfully submits that Cisco does not anticipate Applicant's claimed invention as embodied in claims 3, 6, 8, and 10-13. Claims 3, 6, 8, and 10-13 are allowable for additional reasons. In particular, claim 6 recites that the processor of claim 1 is further operative to receive a second request to add the application, and modify the user's firewall policy to allow at least a portion of the previously

blocked one or more questionable packets associated with the application to pass through the firewall unblocked. Again, Cisco describes that the run-time session controls can be modified at the time the session request is received by the firewall but fails to teach, suggest, or describe a processor operative to modify the run-time session controls to allow at least a portion of the previously blocked one or more questionable packets associated with the session to pass through the firewall unblocked.

Additionally, Cisco fails to teach, suggest, or describe that the one or more questionable packets determined to be included in a session include packets or packet types that are already part of the security policy or packets previously blocked at times other than during the time window but which are now observed during the time window as recited by claim 8. In fact, Cisco fails to teach, suggest, or describe a processor operative to determine whether a session even includes one or more questionable packets. Cisco is also completely silent to the recitations of claims 10-13. Applicant respectfully requests that if Cisco is continued to be used to reject dependent claims 3, 6, 8, and 10-13 that the Office Action particularly point to the sections of Cisco which are being used as support that Cisco allegedly teaches the recitations of these claims. For the above reasons, Applicant respectfully submits that claims 3, 6, 8, and 10-13 are allowable over Cisco. Withdrawal of these rejections is respectfully requested.

Independent claims 16 and 31 include recitations similar to the recitations of claim 1. Thus, for at least the reasons given above with regard to claim 1, claims 16 and 31 are also allowable over Cisco. Since claims 17-28 depend from claim 16 and recite further claim features, Applicant respectfully submits that Cisco does not anticipate Applicant's claimed invention as embodied in claims 17-28. Since claims 32-38, 41-43, and 45 depend from claim 31 and recite further claim features, Applicant respectfully submits that Cisco does not anticipate Applicant's claimed invention as embodied in claims 32-38, 41-43, and 45. Accordingly, Applicant respectfully requests withdrawal of these rejections.

Claim Rejections Under 35 U.S.C. §103

Claims 14-15, 29-30, and 46-53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cisco in view of United States Patent Publication No. 2002/0040396 to Yoshihara et al. (hereinafter "Yoshihara"). This rejection is respectfully traversed.

A. Claims 14-15, 29-30, and 46-47 are allowable.

For at least the reasons given above, claim 1 is allowable over Cisco. As discussed above with regard to claim 1, Cisco fails to teach, suggest, or describe a processor operative to determine whether the application includes one or more questionable packets, and if the application is determined to include one or more questionable packets, modify the user's firewall policy to allow packets associated with the application determined not to be questionable to pass through the firewall unblocked and exclude the one or more questionable packets associated with the application from modification of the user's firewall policy such that the one or more questionable packets are blocked from passing through the firewall.

Similarly, Yoshihara fails to teach, suggest, or describe these recitations of claim 1. In contrast, Yoshihara describes a system that can optimally adjust in real time a policy enforced by a router according to traffic usage such that if too many packets are being discarded during a particular interval by the router, then the policy can be adjusted to increase bandwidth so that less packets are dropped, and if too few packets are being discarded during a particular interval by the router, then the policy can be adjusted to decrease bandwidth so that more packets are dropped. Like Cisco, Yoshihara fails to teach, suggest, or describe a processor operative to determine whether the application includes one or more questionable packets, and if the application is determined to include one or more questionable packets, modify the user's firewall policy to allow packets associated with the application determined not to be questionable to pass through the firewall unblocked and exclude the one or more questionable packets associated with the application from modification of the user's firewall policy such that the one or more questionable packets are blocked from passing through the firewall. Instead, Yoshihara describes that a policy associated with a router may be adjusted to increase or decrease bandwidth to decrease or increase the number of packets dropped by the router, respectively, without teaching or suggesting determining whether the application includes one or more questionable packets, and if the application is determined to include one or more questionable packets, modifying the user's firewall policy to allow packets associated with the application determined not to be questionable to pass through the firewall unblocked and excluding the one or more questionable packets associated with the application from modification of the user's firewall policy such that the one or more questionable packets are blocked from passing through the firewall.

For at least these reasons, claim 1 is allowable over the combined teaching of Cisco and Yoshihara. Since claims 14-15 depend from claim 1 and recite further claim features, Applicant respectfully submits that the combined teaching of Cisco and Yoshihara does not make obvious Applicant's claimed invention as embodied in claims 14-15.

Independent claims 16 and 31 include recitations similar to the recitations of claim 1. Thus, for at least the reasons given above with regard to claim 1, claims 16 and 31 are also allowable over the combined teaching of Cisco and Yoshihara. Since claims 29-30 depend from claim 16 and recite further claim features, Applicant respectfully submits that the combined teaching of Cisco and Yoshihara does not make obvious Applicant's claimed invention as embodied in claims 29-30. Since claims 46-47 depend from claim 31 and recite further claim features, Applicant respectfully submits that the combined teaching of Cisco and Yoshihara does make obvious Applicant's claimed invention as embodied in claims 46-47. Accordingly, Applicant respectfully requests withdrawal of these rejections.

B. Claims 48-53 are allowable.

As amended, claim 48 recites that a system for providing network-based firewall policy configuration and facilitation associated with a firewall comprises a processor, functionally coupled to the memory device, the processor being responsive to computer-executable instructions contained in the program and operative to check packets observed during the time window to be associated with the application to determine whether the packets include one or more questionable packets; when the application is determined to include one or more questionable packets, group the one or more questionable packets by type; prioritize groups of the one or more questionable packets based on a likelihood that the groups will be required to be added to the firewall policy in order to allow the application to function properly; and modify the user's firewall policy to allow packets associated with the application determined not to be questionable to pass through the firewall unblocked and exclude the groups of the one or more questionable packets associated with the application from modification of the user's firewall policy such that the groups of the one or more questionable packets are blocked from passing through the firewall.

Cisco does not teach, suggest, or describe a system for providing network-based firewall policy configuration and facilitation associated with a firewall as recited by claim 48. On the

contrary, Cisco describes a firewall (Cisco Centri Firewall) operative to filter session attempts by evaluating the incoming request to start a new session against session controls and responses defined by a security policy to determine whether to allow the new session. Cisco further describes that the session controls used by the Cisco Centri Firewall to determine whether to allow a new session may be run-time session controls which are session controls that can be modified at the time the session request is received by the firewall and can either apply to all communications or to a specific network service.

This is not analogous to the system recited by claim 48 because Cisco fails to teach, suggest, or describe a processor operative to check packets observed during the time window to be associated with a session to determine whether the packets include one or more questionable packets; when the session is determined to include one or more questionable packets, group the one or more questionable packets by type; prioritize groups of the one or more questionable packets based on a likelihood that the groups will be required to be added to the security policy in order to allow the session to function properly; and modify the security policy to allow packets associated with the session determined not to be questionable to pass through the firewall unblocked and exclude the groups of the one or more questionable packets associated with the session from modification of the security policy such that the groups of the one or more questionable packets are blocked from passing through the firewall. Instead, Cisco describes that the run-time session controls can be modified at the time the session request is received by the firewall but fails to teach, suggest, or describe a processor operative to modify the run-time session controls to allow packets associated with the session determined not to be questionable to pass through the firewall unblocked and exclude the one or more questionable packets associated with the session from modification of the run-time session controls such that the one or more questionable packets are blocked from passing through the firewall. Also, as indicated by the Office Action, Cisco is silent to grouping the one or more questionable packets by type and prioritizing groups of the one or more questionable packets based on a likelihood that the groups will be required to be added to the security policy in order to allow the session to function properly.

The Office Action relies on the teaching of Yoshihara to allegedly cure the above-identified deficiencies of Cisco. However like Cisco, Yoshihara fails to teach, suggest, or describe a system for providing network-based firewall policy configuration and facilitation

associated with a firewall as recited by claim 48. In contrast, Yoshihara describes a system that can optimally adjust in real time a policy enforced by a router according to traffic usage such that if too many packets are being discarded during a particular interval by the router, then the policy can be adjusted to increase bandwidth so that less packets are dropped, and if too few packets are being discarded during a particular interval by the router, then the policy can be adjusted to decrease bandwidth so that more packets are dropped. Yoshihara describes that unconditional droppers discard a packet unconditionally and selective droppers discard selectively a packet under a predetermined condition.

This is not analogous to the system recited by claim 48 because Yoshihara fails to teach, suggest, or describe a processor operative to check packets observed during the time window to be associated with a session to determine whether the packets include one or more questionable packets; when the session is determined to include one or more questionable packets, group the one or more questionable packets by type; prioritize groups of the one or more questionable packets based on a likelihood that the groups will be required to be added to the security policy in order to allow the session to function properly; and modify the security policy to allow packets associated with the session determined not to be questionable to pass through the firewall unblocked and exclude the groups of the one or more questionable packets associated with the session from modification of the security policy such that the groups of the one or more questionable packets are blocked from passing through the firewall. Instead, Yoshihara describes that a policy associated with a router may be adjusted to increase or decrease bandwidth to decrease or increase the number of packets dropped by the router, respectively, without teaching or suggesting checking packets observed during the time window to be associated with an application to determine whether the packets include one or more questionable packets, and modifying the policy to allow packets associated with the application determined not to be questionable to pass through the firewall unblocked and excluding the groups of the one or more questionable packets associated with the application from modification of the policy such that the groups of the one or more questionable packets are blocked from passing through the firewall. Yoshihara describes that packets are discarded either unconditionally or selectively in order to accommodate traffic usage, without teaching or suggesting any determination whether the packets are questionable or any modification of the policy based on any of the packets being determined questionable.

Moreover, Yoshihara fails to teach, suggest, or describe a processor operative to group the one or more questionable packets by type and prioritize groups of the one or more questionable packets based on a likelihood that the groups will be required to be added to the policy in order to allow the application to function properly. As noted above, Yoshihara fails to teach, suggest, or describe any determination whether the packets are questionable or any modification of the policy based on any of the packets being determined questionable. It follows, then, that Yoshihara also fails to teach, suggest, or describe a processor operative to group the questionable packets by type and prioritize groups of the questionable packets based on a likelihood that the groups will be required to be added to the policy in order to allow the application to function properly. In fact, Yoshihara describes that the packets are discarded, which indicates that the packets are no longer available to be prioritized based on a likelihood that the groups will be required to be *added* to the policy in order to allow the application to function properly.

For at least these reasons, claim 48 is allowable over the combined teaching of Cisco and Yoshihara. Since claim 49 depends from claim 48 and recites further claim features, Applicant respectfully submits that the combined teaching of Cisco and Yoshihara does not make obvious Applicant's claimed invention as embodied in claim 49.

Independent claims 50 and 52 include recitations similar to the recitations of claim 48. Thus, for at least the reasons given above with regard to claim 48, claims 50 and 52 are also allowable over the combined teaching of Cisco and Yoshihara. Since claim 51 depends from claim 50 and recites further claim features, Applicant respectfully submits that the combined teaching of Cisco and Yoshihara does not make obvious Applicant's claimed invention as embodied in claim 51. Since claim 53 depends from claim 52 and recites further claim features, Applicant respectfully submits that the combined teaching of Cisco and Yoshihara does make obvious Applicant's claimed invention as embodied in claim 52. Accordingly, Applicant respectfully requests withdrawal of these rejections.

## CONCLUSION

For at least these reasons, Applicant asserts that the pending claims 1, 3, 6, 8, 10-26, 28-38, 41-43, and 45-53 are in condition for allowance. Applicant further asserts that this response addresses each and every point of the Office Action, and respectfully requests that the Examiner pass this application with claims 1, 3, 6, 8, 10-26, 28-38, 41-43, and 45-53 to allowance. Should the Examiner have any questions, please contact Applicant's attorney at 404.815.1900.

Respectfully submitted,

HOPE BALDAUFF HARTMAN, LLC

Date: September 11, 2007

/Jodi L. Hartman/
Jodi L. Hartman
Reg. No. 55,251

Hope Baldauff Hartman, LLC
1720 Peachtree Street, NW
Suite 1010
Atlanta, Georgia 30309
Telephone: 404.815.1900